Probabilistic Characterization of Adversary Behavior in Cyber Security

Carol A. Meyers
(925) 422-1252
meyers14@llnl.gov

Cyber defense is a vast and growing problem in national security. According to the FBI, the annual loss due to cyber crime was estimated at $67.2 billion for U.S. organizations in 2005. Numerous efforts have sought to quantify the impacts of cyber crime, but much less work has focused on characterizing the cyber adversaries themselves. Given that cyber security is such a huge problem, in the construction of a defensive architecture it is essential to know who the cyber adversaries are and what threats they are likely to attempt.

This effort aims to provide a probabilistic characterization of adversary behavior in cyber security, in terms of *who* is perpetuating the attacks and *what methods* they use. The primary data source obtained for this project was a set of unfiltered email data, from a selection of addresses at ciac.org, the former Computer Incident Advisory Capability (CIAC) at LLNL. In addition, we performed an extensive review of the literature in cyber security to address attack vectors for which we were not able to obtain real data.

Project Goals

The objective of this project was to characterize the types of adversaries and attack methods associated with real cyber data, focusing in particular on email as an attack vector. There were three main quantitative thrust areas, centered on analysis of the CIAC dataset: 1) characterization of textual email data; 2) characterization of viruses present in attachments; and 3) characterization of malicious URL content.

The first of these addresses the descriptive content of the emails themselves, such as the volume over time, countries of origin, and methods of spoofing the header data. The second area examines the content of the email attachments, using a suite of antivirus programs to scan the emails and catalogue the kind and frequency of attacks. The third thrust area characterizes the content of web addresses embedded as URLs within the emails (Fig. 1), using custom scripts to query four different online malicious URL detection sites. In the process, we are also able to gauge the relative efficacy of different antivirus and malicious URL detection tools.

Relevance to LLNL Mission

This work directly aligns with the adversary modeling roadmap within the Engineering Systems for Knowledge and Inference (ESKI) portfolio. In addition, it supports the Cyber, Space, and Intelligence mission area of the institutional Science and Technology Five-Year Roadmap to the Future. The capabilities established with this work can be used in future LLNL cyber security studies, particularly in terms of mapping the adversarial threat space. All of the software and tools used are thoroughly documented and available for use by interested parties.

Figure 1. Graphic showing malicious URLs directing users from emails to websites hosting malware content.

FY2009 Accomplishments and Results

The email data used in our characterization was sent between February 2004 and July 2009, with an average of approximately 4000 emails received per month. A reverse lookup of the originating IP addresses was performed to identify the most common associated countries (Fig. 2). China and the United States represented the largest percentage of the sample, followed by South Korea and Brazil.

In terms of the attack methods chosen, we observed that the use of email attachments as an attack vector has decreased sharply over time (Fig. 3). This decrease is probably because email servers have implemented stronger screening procedures and the threat space itself has shifted, due to the lower level of sophistication required to launch an attack using malicious URLs. The number of attacks using malicious URLs increased across the data sample, supporting this hypothesis. With regard to the attacks themselves, the majority of email attachments contained Windows viruses, while most malicious URLs were associated with viruses and drive-by downloads.

Our analyses identified several traits about the adversaries and trends in their behavior. We observed that of the top four countries in the sample, two countries (China and South Korea) also scored very high on maliciousness and low on the trustworthiness of associated emails, while the other two (the United States and Brazil) did not. We can therefore conclude that the largest number of malicious emails is connected with adversaries in Southeast Asia. We also observed that emails sent on weekends are statistically more likely to be malicious than emails sent on weekdays, and the time of day with the highest percentage of malicious activity is late afternoons and evenings.

Finally, we note that the different tools that we used produced dramatically different results. In terms of email attachments, only two of the six tested tools (Norton Antivirus and AVG free) found any threats at all. With respect to malicious URL detection, the Web of Trust tool tested many more domains than any of the other tools (McAfee Site Advisor, Norton SafeWeb, and Google SafeBrowse), and also detected threats in a significantly higher percentage of websites (Fig. 4).

Figure 2. Graphic showing most common countries of origin for emails in the dataset, by reverse IP address lookup. The darker the color intensity, the greater the number of emails received from that country.

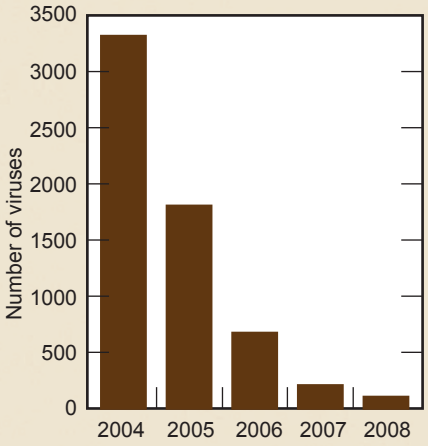

Figure 3. Graphic showing number of viruses identified in emails in the dataset, over time.

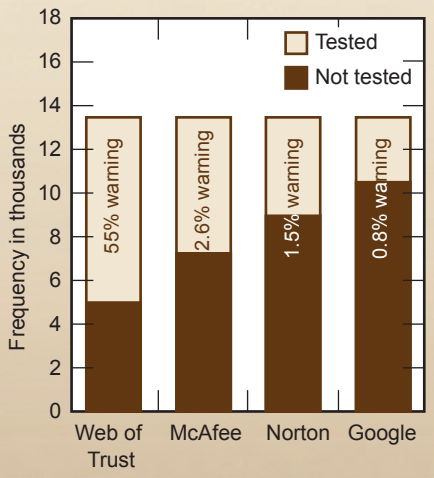

Figure 4. Graphic showing number of domains tested by each of the services, inset with the likelihood that the service generated a warning given a test.

Related References

1. Government Accountability Office (GAO), "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats," *Technical Report GAO-07-705, U.S. Government Accountability Office*, 2007. Accessed at http://www.gao.gov/products/GAO-07-705.
2. Hansman, S., and R. Hunt, "A Taxonomy of Network and Computer Attacks," *Computers and Security*, **21**, pp. 31–43, 2005. Accessed at http://linkinghub.elsevier.com/retrieve/pii/S0167404804001804.
3. Lipson, H., "Tracking and Tracing Cyber Attacks: Technical Challenges and Global Policy Issues," *Technical Report CMU/SEI-2002-SR-009*, Carnegie Mellon University, 2002. Accessed at http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02sr009.pdf.
4. Rantala, R., "Bureau of Justice Statistics Special Report: Cybercrime Against Businesses, 2005," *Technical Report NCJ 221943, U.S. Department of Justice*, 2008. Accessed at http://www.ojp.usdoj.gov/bjs/abstract/cb05.htm.
5. Rogers, M., "A Two-Dimensional Circumplex Approach to the Development of a Hacker Taxonomy," *Digital Investigation*, **3**, pp. 97–102, 2006.